

FIG.5

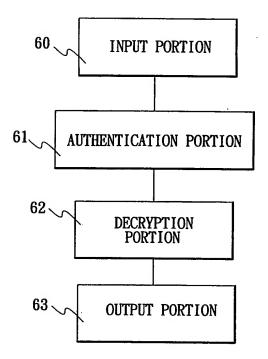


FIG.6

	DATA ATTRIBUTE DESCRIPTION FIELD (24 BYTES)	ENCRYPTION DEFINITION FIELD (8 BYTES)
	DATA ATTRIBUTE DESCRIPTION 1	ENCRYPTION DEFINITION 1
	DATA ATTRIBUTE DESCRIPTION 2	ENCRYPTION DEFINITION 2
L	DATA ATTRIBUTE DESCRIPTION 3	ENCRYPTION DEFINITION 3
<u> </u>		1
	DATA ATTRIBUTE DESCRIPTION N	ENCRYPTION DEFINITION N

FIG.7

	DATA ATTRIBUTE DESCRIPTION	DESCRIPTION			
	COMMAND				
	00	BLANK DATA ATTRIBUTE DESCRIPTION VALUE,			
1		REPRESENTING PREDETERMINED SECURITY CLASS DEFINITION			
-		RECORD LOGIC OPERATOR			
	01 EXPR1 EXPR2	AND OPERATOR EXPR1 AND EXPR2			
	02 EXPR1 EXPR2	OR OPERATOR EXPR1 OR EXPR2			
	03 EXPR1	NOT OPERATOR NOT EXPR2			
		CONDITION EXPRESSION			
	04 AA BBBBBBBB	SOURCE ADDRESS IP IS IDENTICAL WITH THE FIRST AA BYTES OF			
		BBBBBBB			
	05 AA BBBBBBBB	DESTINATION ADDRESS IP IS IDENTICAL WITH THE FIRST AA			
L	0.0	BYTES OF BBBBBBBB			
Ĺ	06 AA	COMMUNICATIONS PROTOCOL VALUE IS AA			
1	07 AAAA BB	DATA AT ADDRESS AAAA, THE ONE-BYTE VALUE THEREOF BEING			
Į		IDENTICAL WITH BB			
ı	08 AAAA BBBB	DATA AT ADDRESS AAAA, THE TWO-BYTE VALUE THEREOF BEING			
		IDENTICAL WITH BBBB			
	09 AAAA BBBBBBBB	DATA AT ADDRESS AAAA, THE FOUR-BYTE VALUE BEING IDENTICAL			
1		WITH BBBBBBBB			
L	0A~FE	RESERVED VALUE			
l	FF	INDICATE THE ENDING VALUE IN DATA ATTRIBUTE			
L		DESCRIPTION FIELD			

## ENCRYPTION ALGORITHM MODULE COMBINATION INDEX VALUE (1 BYTE)

## INDEX 1 PROPORTION 1 INDEX 2 PROPORTION 2 INDEX 3 PROPORTION 3 INDEX 3 PROPORTION 3

PROPORTION VALUE ADOPTED (1 BYTE)

## FIG.9

	DATA ENCRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION	
	ALGORITHM INDICATOR	ALGORITHM INDICATOR	ALGORITHM INDICATOR	
INDEX FIELD(4-BYTE)		FIELD(4-BYTE)	FIELD(4-BYTE)	
1	DATA ENCRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION	
	ALGORITHM INDICATOR 1	ALGORITHM INDICATOR 1	ALGORITHM INDICATOR 1	
2	DATA ENCRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION	
	ALGORTTHM INDICATOR 2	ALGORITHM INDICATOR 2	ALGORITHM INDICATOR 2	
3	DATA ENCRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION	
	ALGORTTHM INDICATOR 3	ALGORITHM INDICATOR 3	ALGORITHM INDICATOR 3	
		,		ユ
N	DATA ENCRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION	
	ALGORTTHM INDICATOR N	ALGORITHM INDICATOR N	ALGORITHM INDICATOR N	

## FIG. 10

INDEX	DATA DECRYPTION ALGORITHM INDICATOR ( FIELD(4-BYTE)	DATA AUTHENTICATION ALGORITHM INDICATOR FIELD(4-BYTE)	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR FIELD(4-BYTE)
1	DATA DECRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION
	ALGORITHM INDICATOR 1	ALGORITHM INDICATOR 1	ALGORITHM INDICATOR 1
2	DATA DECRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION
	ALGORITHM INDICATOR 2	ALGORITHM INDICATOR 2	ALGORITHM INDICATOR 2
3	DATA DECRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION
	ALGORITHM INDICATOR 3	ALGORITHM INDICATOR 3	ALGORITHM INDICATOR 3
`			,
N	DATA DECRYPTION	DATA AUTHENTICATION	INTEGRATED AUTHENTICATION
	ALGORITHM INDICATOR N	ALGORITHM INDICATOR N	ALGORITHM INDICATOR N

FIG.11

	HEADE	CR		DATA			
					_		
0		4	8	16	20	243	Bit
	VERS	HLEN	SERVICE TYPE	;		TOTAL LENGTH	7
	IDENT	'IFICATIO	V	FLAGS		FRAGMENT OFFSET	1
	TIME	TO LIVE	PROTOCOL			HEADER CHECKSUM	
	SOURCE IP ADDRESS						
	DESTINATION IP ADDRESS						1
	IP OPTIONS (IF ANY) PADDING						
						1	
1	32 Bits					-	

FIG.12

HEADER	DECRYPTION INFORMATION DA	TA CIPHERTEXT DATA			
	DECRYPTION INFORMATION LABEL	DECRYPTION MODULE DATABASE INDEX			

FIG.13

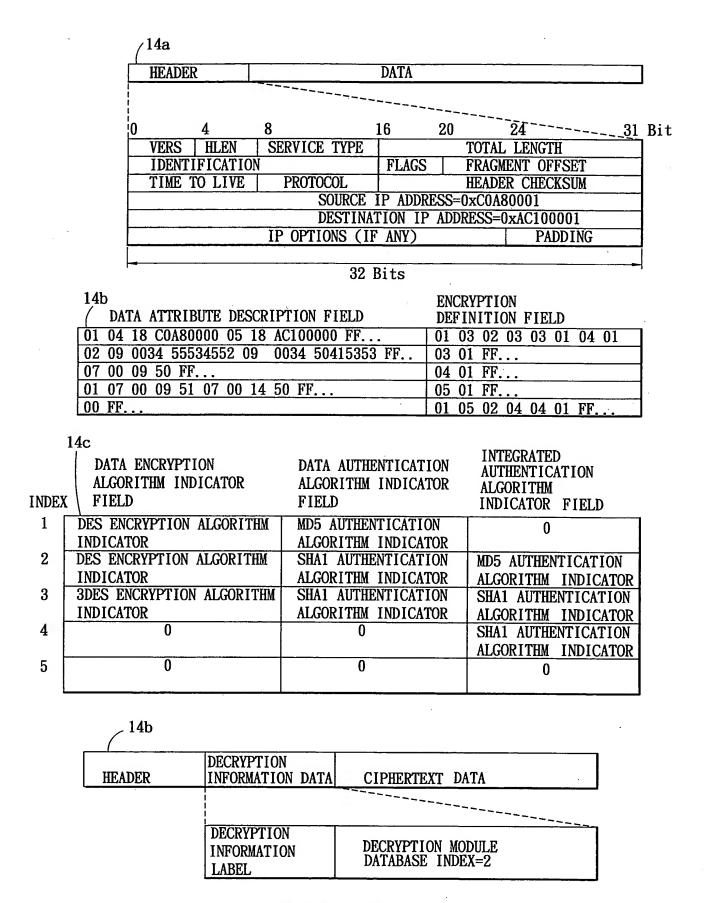


FIG.14

DECRYPTION CIPHERTEXT DATA

DECRYPTION DECRYPTION DECRYPTION MODULE DATABASE INDEX=2

INDEX	15b DATA DECRYPTION ALGORITHM INDICATOR FIELD	DATA AUTHENTICATION ALGORITHM INDICATOR FIELD	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR FIELD
. 1	DES DECRYPTION ALGORITHM	MD5 AUTHENTICATION	0
	INDICATOR	ALGORITHM INDICATOR	,
2	DES DECRYPTION ALGORITHM	SHA1 AUTHENTICATION	MD5 AUTHENTICATION
	INDICATOR	ALGORITHM INDICATOR	ALGORITHM INDICATOR
3	DES DECRYPTION ALGORITHM	SHA1 AUTHENTICATION	SHA1 AUTHENTICATION
	INDICATOR	ALGORITHM INDICATOR	ALGORITHM INDICATOR
4	0	0	SHA1 AUTHENTICATION
į			ALGORITHM INDICATOR
5	0	0	0

HEADER PLAINTEXT DATA

FIG.15

